



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,282	02/14/2000	Dung Le Huynh	230074-0223	6335

7590 06/06/2003

Ted R Rittmaster Esq  
Foley & Lardner  
2029 Century Park East  
Suite 3500  
Los Angeles, CA 90067-3021

EXAMINER

SONG, HOSUK

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 06/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.  
09/503,282

Applicant(s)  
HUYNH ET AL.

Examiner  
HOSUK SONG

Art Unit  
2131



-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on Mar 21, 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above, claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-42 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claims \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some\* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\*See the attached detailed Office action for a list of the certified copies not received.

- 14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).  
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). \_\_\_\_\_ 6) ☐ Other:

Art Unit: 2131

### DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/21/03 has been entered.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 5-8,15,22,29,35 are rejected under 35 U.S.C. 103(a) as being unpatentable by Wu et al.(US 5,774,551) in view of Candelore et al.(US 6,061,449) or Anderson(US 5,911,077) .

In claims 5,22,35 Wu discloses a control unit having a data input bus (fig.1). Encryption processing unit in (col.3, lines 58-62). First and second authentication processing unit in (col.8, lines 61-66). A local data bus, independent of the data input bus to the control unit, coupling the control unit to each of the encryption and authentication processing units and a second data bus from the encryption unit to each authentication unit, including a data bus from the first authentication processing unit to the second authentication processing unit in (fig.1 #115,109,123

Art Unit: 2131

and col.3, lines 56-66). Wu does not disclose where data is provided to at least one encryption unit processing unit and processed by the at least one encryption processing unit while at least one authentication processing unit is further processing output data from one data packet. Candelore disclose concurrent processing in (fig.1 and fig.6). Anderson disclose concurrent processing method where plurality of packets are processed concurrently for different tasks in (col.11, lines 6-41). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ concurrent processing disclosed in Candelore or Anderson with encryption unit disclosed in Wu in order for data packet to continuously flow without delay thus reducing computer downtime. Further concurrent processing allows second packet to be processed quickly thus achieving immediate validation. It overall enhances speed of data processing.

In claim 6, Wu disclose wherein data input bus of the control unit is coupled to a processor bus and each of encryption and authentication processing units comprises a data input bus coupled to the processor bus in (fig.1, #109, 123).

In claim 7, Wu discloses first authentication unit and second authentication processing unit in (col.8, lines 61-65).

In claim 8, Wu discloses all the limitations above. However, Wu does not discloses second data bus comprising a daisy-chain connection between the encryption and authentication processing units. The examiner takes Official notice that chain is well known in the art. It is widely used in order to eliminate conflicting requests to use the channel(bus) to which all the devices are connected, each device is given a different priority.

Art Unit: 2131

In claims 15,29, Wu discloses an encrypting a first packet with an encryption processing module and authenticating the encrypted first data packet with a first authentication processing module in (fig.1 and col.3, lines 56-62; col.15, lines 54-67). Wu does not specifically disclose encrypting a second data packet with the encryption processing module while authenticating the first data packet with the first authentication processing module connected to the encryption processing module by a data bus and authenticating the second data packet with the first authentication processing module. Candelore disclose concurrent processing in (fig.1 and col.14,lines 8-12). Anderson disclose concurrent processing method where plurality of packets are processed concurrently for different tasks in (col.11,lines 6-41) It would have been obvious to person of ordinary skill in the art at the time invention was made to employ concurrent processing disclosed in Candelore/Anderson with encryption unit disclosed in Wu in order for data packet to continuously flow without delay thus reducing computer downtime. Further concurrent processing allows second packet to be processed quickly thus achieving immediate validation. It overall enhances speed of data processing.

4. Claims 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable by Wu et al.(US 5,774,551) in view of Candelore et al.(US 6,061,449) or Anderson(US 5,911,077) and further in view of Kocher et al.(US 6,304,658) .

Claims 32,33,34: Wu,Candelore,Anderson does not disclose HMAC-key hashing. Kocher patent disclose HMAC-key hashing method in (col.9,lines 1-16). It would have been obvious to person of ordinary skill in the art at the time invention was made to use HMAC-key hashing

Art Unit: 2131

method disclosed in Kocher with packet processor system taught in WU, Candelore, Anderson because HMAC is designed to be resistant to differential analysis. Since HMAC hashes a known value with an unknown value and the result of this hash is then rehashed with a separate unknown value, making any differential attack extremely difficult.

5        Claims 1-4, 9-14, 16-21, 23-28, 30-31, 36-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wu et al. (US 5,774,551).

In claims 1-2, 9, 16, 23, 30, 36-42, Wu discloses encrypting and authenticating a first packet and discloses two authentication services connected to the encryption unit by a data bus in (fig. 1 and col. 15, lines 53-67). Wu does not specifically disclose performing encryption on a first data packet and after completion of the encryption of the first data packet, performing authentication of the first packet and performing encryption of a second data packet prior to completion of authentication of the first data packet. The examiner takes Official notice that encrypting a second packet before authentication is well known in the art. For example, parallel encryption scheme where first and second packets are encrypted at the same time where second packet does not wait for first packet to be authenticated thus allowing faster encryption/authentication process when transmitting over the network or encrypting a second packet before first packet is authenticated or encrypting a second packet while authenticating first packet eliminates waiting time thus enhances encryption /authentication processing speed.

Art Unit: 2131

In claim 3, Wu discloses data input bus of the control unit is coupled to a processor bus and each of encryption and authentication processing units comprises a data input bus to the processor bus and means for reading and writing data on the processor bus in (see fig.3).

In claim 4, Wu discloses all the limitations above. However, Wu does not disclose second data bus comprising a daisy-chain connection between the encryption and authentication processing units. The examiner takes Official notice that chain is well known in the art. It is widely used in order to eliminate conflicting requests to use the channel(bus) to which all the devices are connected, each device is given a different priority.

In claim 10,17, Wu discloses step of performing a second authentication on the first data packet of data in (col.7, table 1).

In claims 11-14,18-21, Wu discloses appending data to first authentication and second authentication in (col.3, lines 56-66).

In claims 24-28 see claims rejection 10-14 above.

In claim 31 see claims rejection 23 above.

### ***Conclusion***

6 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. .

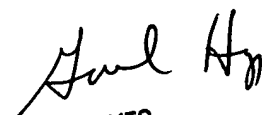
- a. Eide et al.(US 6,243,774) disclose concurrent processing by a system.
- b. Likens et al.(US 5,631,960) disclose cryptographic packet processor.

Art Unit: 2131

7 Any inquiry concerning this communication should be directed to Hosuk. Song whose telephone number (703)305-0042. The examiner can normally be reached on Tuesday through Friday from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached at (703)305-9711.

Any inquiry of a general nature or relating to the status of this application or preceding should be directed to the Group receptionist, whose telephone number is (703)305-3900.



GAIL HAYES  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100